NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

ENCAPSULATION NIVEAU 2

Produits concernés : SNS 4.x

Dernière mise à jour du document : 22 mars 2021

Référence : sns-fr-encapsulation_niveau_2_note_technique

Table des matières

Avant de commencer

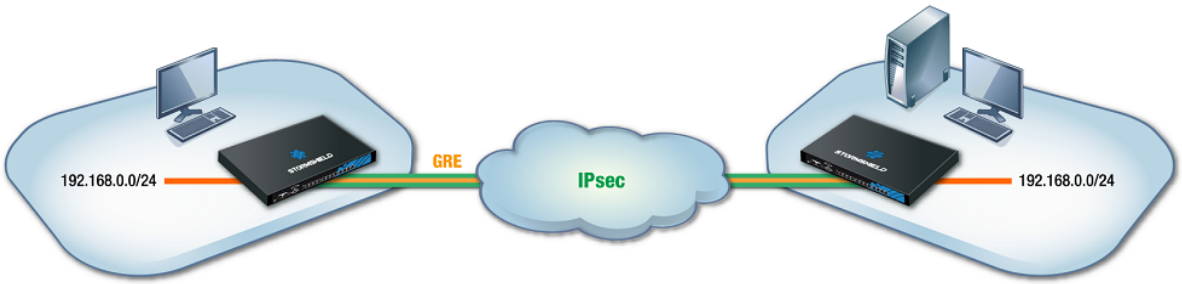
Les firewalls SNS peuvent encapsuler des flux de niveau 2 dans des tunnels GRE (Generic Routing Encapsulation) basés sur des interfaces GRETAP. Les tunnels GRE n'étant pas chiffrés nativement, il est fortement conseillé de sécuriser les échanges en faisant transiter les flux GRE au travers d'IPsec.

L'utilisation de tunnels GRE basés sur des interfaces GRETAP permet par exemple de relier au travers d'un bridge des sites présentant le même plan d'adressage. Des services de type DHCP peuvent ainsi être partagés entre les deux sites. Ce type de tunnel permet également de transporter entre deux sites des VLAN partagés, avec ou sans filtrage sur ces VLAN.

IMPORTANT
L'utilisation de tunnels GRE est possible uniquement avec des paquets IPv4 dans des tunnels GRE encapsulés dans de l'IPv4. Les cas utilisant des paquets IPv6 dans des tunnels GRE ou des tunnels GRE encapsulés dans de l'IPv6 ne sont pas supportés.

Architectures présentées

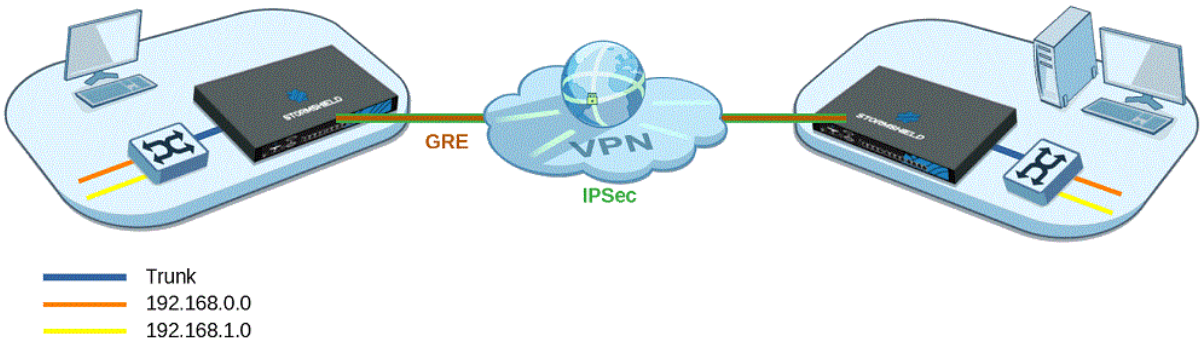
Cas N°1 : réunion de deux sites partageant le même plan d'adressage



Cette section présente le cas d'une entreprise souhaitant relier au travers d'un bridge deux sites partageant un plan d'adressage identique. Les services, DHCP par exemple, et les ressources réseau partagées seront ainsi vus comme des services locaux, quel que soit le site. Pour sécuriser ces échanges, les flux GRE seront chiffrés dans un tunnel IPsec.

NOTE
Les adresses IP attribuées aux équipements des deux sites doivent bien évidemment être uniques.

Cas N°2 : transport de plusieurs VLAN dans un tunnel GRE sans filtrage / routage inter-VLAN



Cette section présente le cas d'une entreprise souhaitant partager plusieurs VLAN entre deux sites au travers d'un tunnel GRE sécurisé par du chiffrement (IPsec).
Cette configuration **autorise des communications inter VLAN au travers du tunnel GRE**.

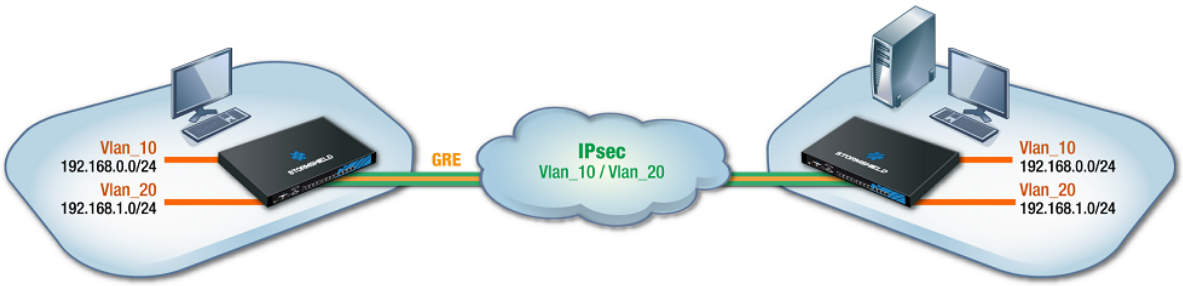
Dans cette architecture, les VLAN ne sont pas déclarés sur les firewalls : aucune opération spécifique basée sur les interfaces VLAN ne peut donc être appliquée et tous les VLAN sont implicitement autorisés à emprunter le tunnel GRE.
Seuls les réseaux IP associés aux VLAN sont connus du firewall et peuvent faire l'objet de filtrage spécifique par exemple.

Le routage est réalisé par des commutateurs de niveau 3 situés sur le LAN de chacun des sites. Dans cette configuration, le lien entre les firewalls et les commutateurs est un lien de type Trunk et l'ensemble des tags de VLAN est renvoyé dans le tunnel.

Sont abordés la création des interfaces GRETAP et le paramétrage des interfaces physiques associées aux interfaces GRETAP (paramètres avancés **Préserver les identifiants de VLAN** et **Préserver le routage initial**) ainsi que la création du tunnel IPsec.

IMPORTANT
Si votre configuration nécessite que du filtrage spécifique puisse être appliqué aux VLAN avant d'emprunter le tunnel GRE, veuillez consulter la section Cas N°3.
Notez que ce cas peut être appliqué à une architecture comportant plus de deux firewalls (architecture en étoile), mais en aucun cas dans le cadre d'une topologie complètement maillée (full mesh).

Cas N°3 : transport de VLAN dans un tunnel GRE avec filtrage de VLAN



Cette section présente le cas d'une entreprise souhaitant partager deux VLAN entre deux sites au travers d'un tunnel GRE sécurisé par du chiffrement (IPsec).
Cette architecture **n'autorise pas les communications inter VLAN au travers du tunnel GRE**.

Y sont abordés la configuration propre à la création des interfaces GRETAP, au tunnel IPsec, au paramétrage des VLAN et à leur rattachement aux interfaces GRETAP.

L'association d'un bridge à chaque VLAN permet le filtrage des VLAN au travers du tunnel : seuls les VLAN déclarés sur les firewalls sont autorisés à transiter au travers du tunnel.

IMPORTANT

- Cette configuration génère du routage entre les VLAN transportés dans le tunnel et entraîne une détection d'usurpation d'adresses (*IP spoofing*) par l'un des firewalls portant le tunnel GRE si des machines issues des deux VLAN tentent de communiquer entre elles au travers du tunnel.
  Si votre configuration nécessite des communications inter VLAN, veuillez consulter la section Cas N°2.
- Un bridge étant utilisé pour chaque VLAN transporté, il est donc essentiel de s'assurer que le firewall supporte le nombre de bridges envisagés.

La commande `system property` (module **Configuration** > **Système** >**Console CLI**) permet de recueillir le nombre de bridges supportés par le firewall :

SYSTEM / CLI

```
SYSTEM      : System commands
USER        : User related functions
VERSION     : Display server version
system property
[Result]
Type=Firewall
Model=EVAU
MachineType=amd64
Version=[redacted]
ASQVersion=9.0.0
SerialNumber=[redacted]
MTUmax=9198
LACP=0
Bridge=8
```

Cas N°1 : réunion de deux sites partageant le même plan d'adressage

Créer l'interface GRETAP

Sur chacun des firewalls participant au tunnel GRETAP, dans le module **Configuration** > **Réseau** > **Interfaces** :

1. Cliquez sur **Ajouter.**
2. Choisissez **Interface GRETAP**.
   La fenêtre de configuration de l'interface s'affiche.
3. Dans l'onglet **Configuration Générale** > **Paramètres généraux** :
   - Affectez un **Nom** à l'interface GRETAP (*gretap_FW* dans l'exemple).
   - Dans le champ **Cette interface est**, sélectionnez **interne (protégée)**.
4. Dans l'onglet **Configuration Générale** > **Adresses du tunnel GRETAP** :
   - **Source du tunnel** : sélectionnez l'interface physique par laquelle les flux GRE transiteront en sortie du Firewall. Dans l'exemple présenté, il s'agit de l'interface **Firewall_out**.
   - **Destination du tunnel** : sélectionnez un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).
5. Dans l'onglet **Configuration Générale** > **Plan d'adressage** :
   - Cochez **Plan d'adressage hérité du bridge,**
   - Sélectionnez ensuite le **Bridge** auquel l'interface doit être rattachée.
     Il peut s'agir du bridge issu de la configuration par défaut ou d'un bridge créé pour cet usage.

> **NOTES**
>
> - Il n'est pas possible de créer un bridge au sein de l'assistant de création de l'interface GRETAP.
> - Il est possible de ne pas sélectionner de bridge pour l'interface GRETAP en forçant l'état de l'interface à OFF. L'interface pourra alors être activée ultérieurement en la déplaçant dans un bridge.

6. Cliquez sur **Appliquer** pour valider la création de l'interface GRETAP.

Créer le tunnel IPsec

Sur chacun des firewalls participant au tunnel GRETAP, dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - Tunnels** :

1. Cliquez sur le bouton **Ajouter.**
2. Sélectionnez **Tunnel site à site**.
3. Pour le champ **Réseau local** : sélectionnez l'interface physique portant le tunnel GRE (**Firewall_out** dans l'exemple).
4. Pour le champ **Réseau distant** : sélectionnez un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).

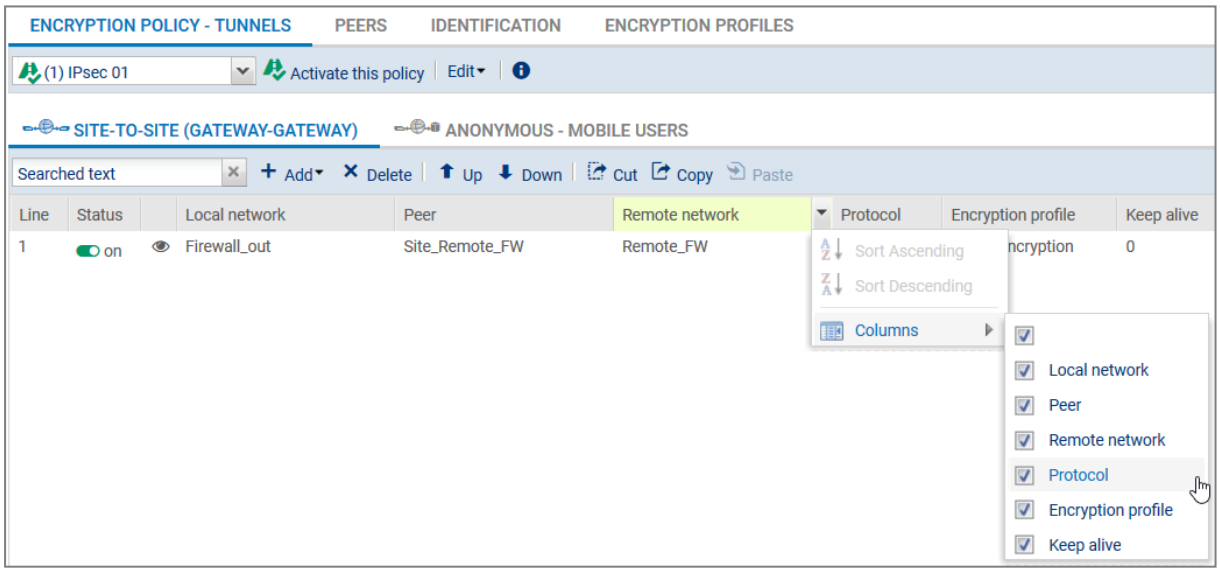
5. Pour le champ **Choix du correspondant** : créez (ou sélectionnez le s'il existe déjà) un correspondant dont la passerelle distante sera un objet portant l'adresse IP publique du Firewall distant.
6. Cliquez sur **Terminer**.

NOTES
Pour plus de détails concernant la création d'un correspondant utilisant les méthodes d'authentification par clé pré-partagée ou par certificats, veuillez consulter les documents VPN IPsec - Authentification par clé pré-partagée et VPN IPsec - Authentification par certificats.

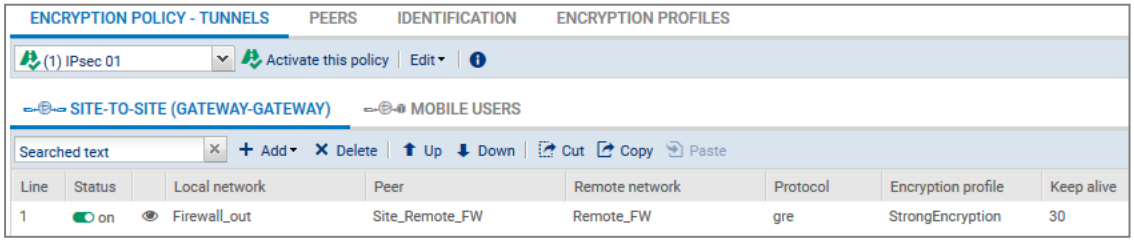
La version du protocole IKE pour ce correspondant doit être identique à :

- Celle utilisée sur le firewall distant,
- Celle des correspondants utilisés dans les autres règles de la politique IPsec concernée.

7. Afin de ne pas autoriser l'établissement du tunnel IPsec pour des protocoles autres que GRE et éviter le chiffrement de flux tels que ICMP (*Ping*), il est conseillé de spécifier le protocole GRE dans la colonne **Protocole**.
Si cette colonne n'est pas affichée, passez votre souris sur le titre d'une colonne quelconque et déroulez le menu contextuel en cliquant sur la flèche. Sélectionnez **Colonne** puis cochez **Protocole**.



La politique VPN IPsec prendra donc la forme suivante :



NOTE
Le firewall étant à l'initiative de l'émission des paquets réseau GRE, il n'est donc pas nécessaire de créer de règles de filtrage pour ce protocole.

Vérifier les tunnels

Tunnel GRE

Pour vérifier le fonctionnement du tunnel GRE non chiffré entre les deux Firewalls :

1. Désactivez la règle IPsec sur chaque site en mettant son état à **off.**
2. Activez la politique IPsec.
3. Depuis un poste situé sur le réseau local du site A, lancez un test de disponibilité (*Ping*) vers une machine située sur le réseau local du site B.
   Cette machine doit répondre aux requêtes.

Tunnel GRE chiffré dans un tunnel IPsec

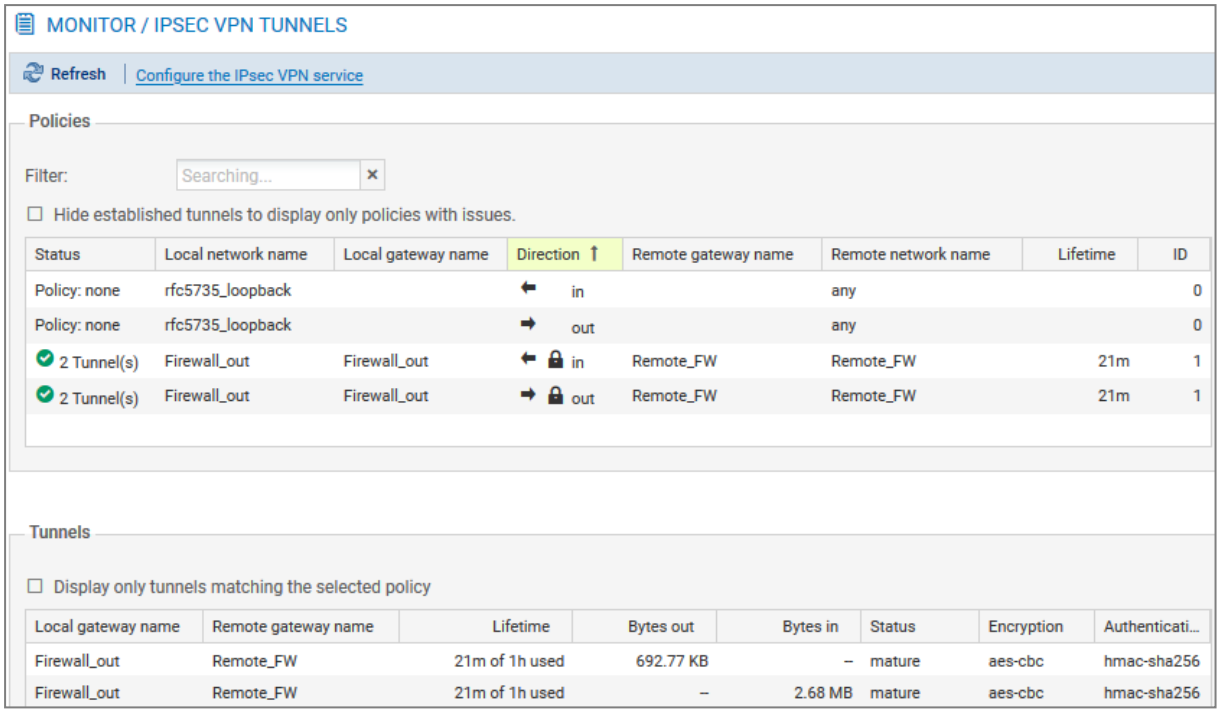
Sur chaque Firewall :

1. Activez la règle IPsec en fixant son état à **on :**
2. Activez la politique IPsec.
3. Depuis un poste situé sur le réseau local du site A, lancez un test de disponibilité (*Ping*) d'une machine située sur le réseau local du site B.
   Cette machine doit répondre aux requêtes.

Vérification depuis l'interface Web des Firewalls

Dans l'interface Web d'administration des firewalls, cliquez sur **Monitoring** > **Supervision** **Tunnels VPN IPsec**.
La fenêtre affiche les tunnels établis ainsi que le détail de ces tunnels :

- Nom de l'extrémité locale du tunnel,
- Nom de l'extrémité distante du tunnel,
- Durée de vie,
- Octets entrants,
- Octets sortants,
- État du tunnel
- Algorithme de chiffrement utilisé,
- Algorithme d'authentification utilisé.



Les traces concernant l'établissement du tunnel IPsec peuvent être consultées dans l'onglet **Monitoring** > **Logs - Journaux d'audit** > **VPN**.

Cas N°2 : transport de VLAN dans un tunnel GRE avec routage inter-VLAN délégué

Avant de commencer cette configuration, il est important de noter que cette configuration ne permet pas de réaliser de filtrage sur les VLAN transportés dans le tunnel GRE. Si votre configuration nécessite que le filtrage de VLAN soit assuré, veuillez consulter la section Cas N°3.

Avant de commencer

Pour mettre en place l'infrastructure proposée, la configuration de chaque firewall participant au tunnel GRETAP / IPsec se décompose en 5 étapes :

- Créer le bridge destiné à l'interface GRETAP,
- Choisir et vérifier le paramétrage additionnel de l'interface physique qui sera associée à l'interface GRETAP (interface *in* dans cet exemple),
- Créer et paramétrer l'interface GRETAP,
- Regrouper ces deux interfaces dans le bridge dédié au tunnel GRETAP,
- Définir le tunnel IPsec.

Créer le bridge pour l'interface GRETAP

Sur chacun des firewalls participant au tunnel GRETAP, dans le module **Configuration** > **Réseau** > **Interfaces** :

1. Cliquez sur **Ajouter** puis choisissez **Bridge** > **Sans membre**.
   Un bridge nommé par défaut *new_bridge1* est créé.
   Ce nom pourra être personnalisé par la suite.
2. Dans l'onglet **Configuration générale** > **Plan d'adressage**, sélectionnez, selon votre configuration réseau, **IP dynamique (obtenue par DHCP)** ou **IP fixe** pour donner au bridge une adresse IP dans le réseau d'accès à Internet.
3. Cliquez sur **Appliquer**.
4. Confirmez en cliquant sur **Sauvegarder**.

Créer et activer l'interface GRETAP

Sur chacun des firewalls participant au tunnel GRETAP, dans le module **Configuration** > **Réseau** > **Interfaces** :

1. Cliquez sur **Ajouter.**
2. Sélectionnez **Interface GRETAP**.
   La fenêtre de configuration de l'interface s'affiche.
3. Placez-vous dans l'onglet **Configuration générale.**
4. Dans la partie **État**, placez le curseur sur **ON**.
5. Dans la partie **Paramètres généraux** > champ **Nom**, nommez l'interface GRETAP (*GretapVLAN* dans l'exemple).
6. Dans la partie **Paramètres généraux** > champ **Cette interface est**, cochez la case **Externe (publique)**.

7. Dans la partie **Adresses du tunnel GRETAP** > champ **Source du tunnel** : sélectionnez l'interface physique par laquelle les flux GRE transiteront en sortie du Firewall pour emprunter le tunnel IPsec.
   Dans l'exemple présenté, il s'agit de l'interface **Firewall_out**.
8. Dans la partie **Adresses du tunnel GRETAP** > champ **Destination du tunnel** : sélectionnez (ou créez) un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).
9. Dans la partie **Plan d'adressage** > champ **Adressage**, sélectionnez **Plan d'adressage hérité du bridge**.
10. Dans la partie **Plan d'adressage** > champ **Bridge**, sélectionnez le bridge précédemment créé (*new_bridge1* dans l'exemple).
    L'interface est automatiquement placée dans le bridge *new_bridge1*.
11. Placez-vous dans l'onglet **Configuration avancée.**
12. Dans la section **Routage par interface**, cochez la case **Préserver le routage initial**.
    Une case **Préserver les identifiants de VLAN** apparaît. Cochez-là.
13. Cliquez sur **Appliquer** puis **Sauvegarder** pour valider la création de l'interface GRETAP.

Modifier le paramétrage de l'interface physique source du trafic et la déplacer dans le bridge

Sur chacun des firewalls participant au tunnel GRETAP :

1. Dans le module **Configuration** > **Réseau** > **Interfaces**, faites un double clic sur l'interface physique source du trafic devant transiter dans le tunnel.
   Dans l'exemple présenté, il s'agit de l'interface **in**.
2. Dans la partie **Paramètres généraux** > champ **Cette interface est**, cochez la case **Externe (publique)**.
3. Dans la partie **Plan d'adressage** > champ **Adressage**, sélectionnez **Plan d'adressage hérité du bridge**.
4. Dans la partie **Plan d'adressage** > champ **Bridge**, sélectionnez le bridge précédemment créé (*new_bridge1* dans l'exemple).
   L'interface est automatiquement déplacée dans le bridge *new_bridge1*.
5. Placez-vous dans l'onglet **Configuration avancée.**
6. Dans la section **Routage par interface**, cochez la case **Préserver le routage initial**.
   Une case **Préserver les identifiants de VLAN** apparaît. Cochez-là.
7. Cliquez sur **Appliquer** pour valider la création de l'interface GRETAP.

Renommer le bridge (optionnel)

Si vous souhaitez modifier le nom du bridge dans lequel a été placée l'interface GRETAP, dans le menu **Configuration** > **Réseau** > **Interfaces**, faite un double clic sur ce bridge (*new_bridge1* dans cet exemple) :

1. Dans l'onglet **Configuration Générale** > **Paramètres généraux** > champ **Nom**, donnez un nouveau nom au bridge (*gretap_bridge* dans l'exemple).
2. Cliquez sur **Appliquer** puis sur **Sauvegarder**.

Créer le tunnel IPsec

Sur chacun des firewalls participant au tunnel GRETAP, dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - Tunnels** :

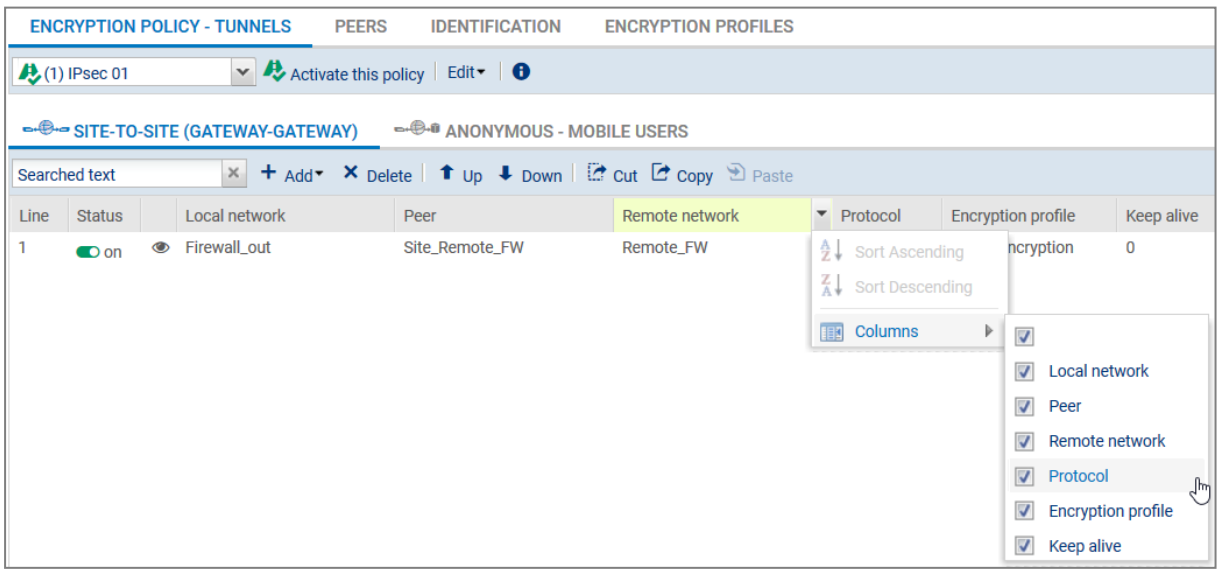
1. Cliquez sur le bouton **Ajouter.**
2. Sélectionnez **Tunnel site à site**.
3. Pour le champ **Réseau local** : sélectionnez l'interface physique portant le tunnel GRE (**Firewall_out** dans l'exemple).
4. Pour le champ **Réseau distant** : sélectionnez un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).
5. Pour le champ **Choix du correspondant** : créez (ou sélectionnez-le s'il existe déjà) un correspondant dont la passerelle distante sera un objet portant l'adresse IP publique du Firewall distant.
6. Cliquez sur **Terminer**.

NOTES
Pour plus de détails concernant la création d'un correspondant utilisant les méthodes d'authentification par clé pré-partagée ou par certificats, veuillez consulter les documents VPN IPsec - Authentification par clé pré-partagée et VPN IPsec - Authentification par certificats.

La version du protocole IKE pour ce correspondant doit être identique à :

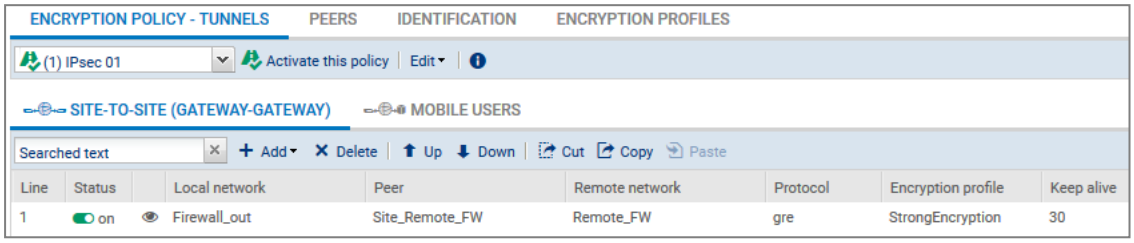
- Celle utilisée sur le firewall distant,
- Celle des correspondants utilisés dans les autres règles de la politique IPsec concernée.

7. Afin de ne pas autoriser l'établissement du tunnel IPsec pour des protocoles autres que GRE et éviter le chiffrement de flux tels que ICMP (*Ping*), il est conseillé de spécifier le protocole GRE dans la colonne **Protocole**.
   Si cette colonne n'est pas affichée, passez votre souris sur le titre d'une colonne quelconque et déroulez le menu contextuel en cliquant sur la flèche. Sélectionnez **Colonnes** puis cochez **Protocole**.



8. Pour permettre au tunnel de s'établir sans flux initial et de rester établi même lorsque le trafic s'interrompt pour une courte période, cliquez dans la colonne **Keepalive** et choisissez une durée (30 secondes dans l'exemple).

La politique VPN IPsec prendra donc la forme suivante :



NOTE
Le firewall étant à l'initiative de l'émission des paquets réseau GRE, il n'est donc pas nécessaire de créer de règles de filtrage pour ce protocole.

Vérifier le fonctionnement

Depuis une machine du site A appartenant à l'un des VLAN, faites un test de disponibilité (*Ping*) vers une machine du site B appartenant au même VLAN : la machine du site B doit répondre aux requêtes.

Il est également possible de vérifier que les VLAN sont bien transportés dans le tunnel en effectuant une capture réseau sur l'interface d'entrée du tunnel du firewall du site B. Dans ce cas, les paquets réseaux capturés laissent ainsi apparaître le protocole GRE encapsulant le VLAN transporté (VLAN 20 dans l'exemple):

```
15:41:06.019669 00:90:fb:2c:5d:b2 > 00:0d:b4:0c:c6:b6, ethertype IPv4 (0x0800), length 108: 172.16.3.1 > 172.16.2.1: GREv0,
proto TEB (0x6558), length 74: 18:03:73:8b:51:d8 > 01:00:5e:00:00:fc, ethertype 802.1Q (0x8100), length 70: vlan 20, p 0,
ethertype IPv4, 192.168.1.10.50677 > 224.0.0.252.5355: UDP, length 24
```

Cas N°3 : transport de VLAN dans un tunnel GRE avec filtrage de VLAN

Avant de commencer cette configuration, il est important de noter que :

- Cette configuration ne permet pas de réaliser de routage entre les VLAN transportés dans le tunnel GRE. Si votre configuration nécessite que le routage entre les VLAN soit assuré, veuillez consulter la section Cas N°2.
- Un bridge est nécessaire pour chaque VLAN transporté. Il est donc essentiel de s'assurer que le firewall supporte le nombre de bridges envisagés.
- Cette association bridge / VLAN permet le filtrage des VLAN au travers du tunnel : seuls les VLAN associés aux bridges sont en effet autorisés à transiter au travers du tunnel.

Avant de commencer

Pour mettre en place l'infrastructure proposée, la configuration de chaque firewall participant au tunnel GRETAP / IPsec se décompose en 4 étapes :

- Créer et paramétrer l'interface GRETAP,
- Créer les VLAN,
- Regrouper ces VLAN dans un bridge dédié,
- Définir le tunnel IPsec.

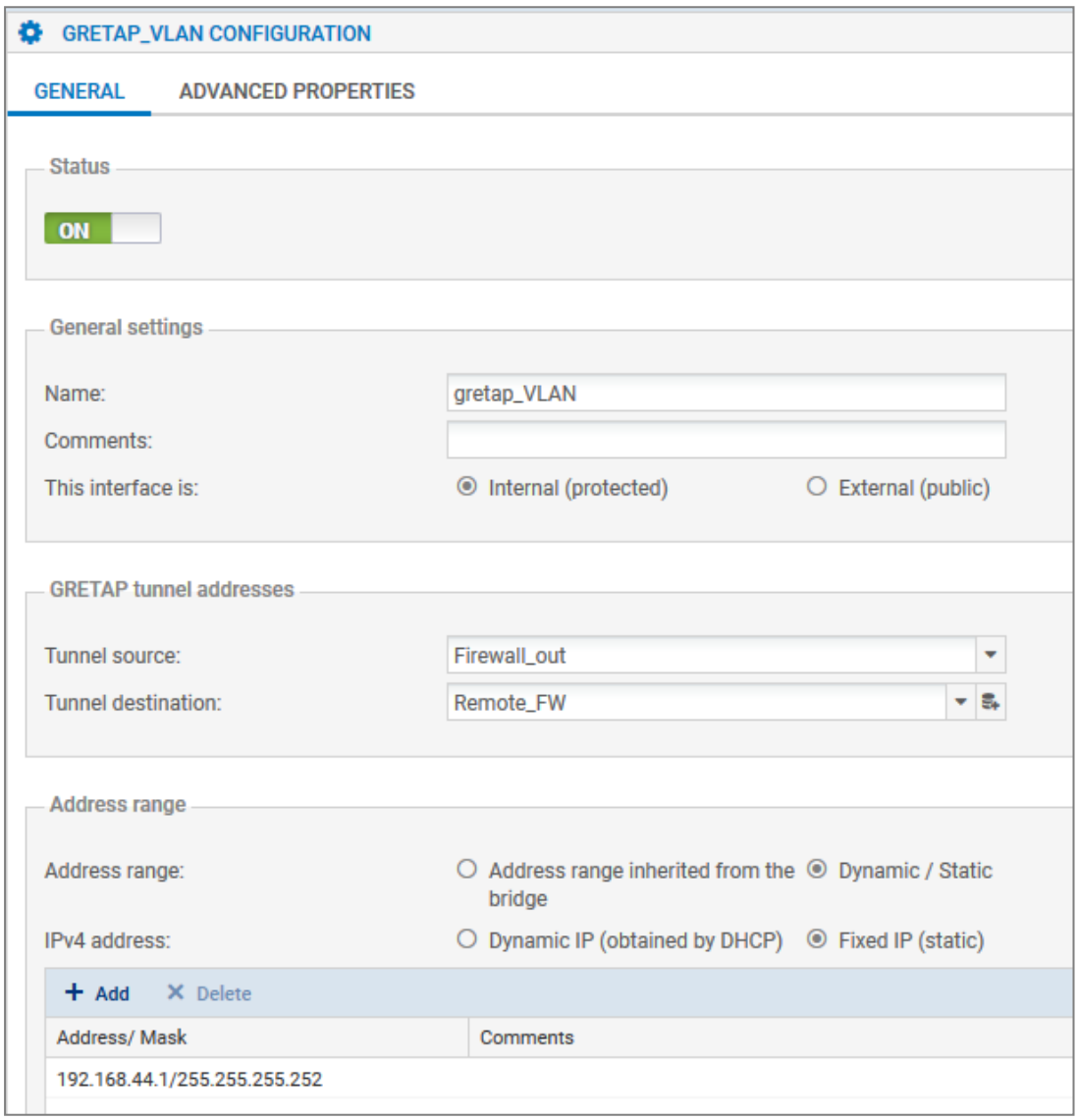
Créer et activer l'interface GRETAP

Sur chacun des firewalls participant au tunnel GRETAP, dans le module **Configuration** > **Réseau** > **Interfaces** :

1. Cliquez sur **Ajouter.**
2. Sélectionnez **Interface GRETAP**.
   La fenêtre de configuration de l'interface s'affiche.
3. Placez-vous dans l'onglet **Configuration Générale.**
4. Dans la partie **État**, placez le curseur sur **ON.**
5. Dans la partie **Paramètres généraux** > champ **Nom**, nommez l'interface GRETAP (GretapVLAN dans l'exemple).
6. Dans la partie **Paramètres généraux** > champ **Cette interface est**, cochez la case **Externe (publique)**.
7. Dans la partie **Adresses du tunnel GRETAP** > champ **Source du tunnel** : sélectionnez l'interface physique par laquelle les flux GRE transiteront en sortie du firewall. Dans l'exemple présenté, il s'agit de l'interface **Firewall_out**.
8. Dans la partie **Adresses du tunnel GRETAP** > champ **Destination du tunnel** : sélectionnez (ou créez) un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).
9. Dans la partie **Plan d'adressage** > champ **Adressage**, sélectionnez l'option **Dynamique / Statique**.

NOTE
Ne pas rattacher l'interface GRETAP à un bridge permet de n'autoriser dans le tunnel GRE que les paquets réseau des VLAN rattachés à cette interface (VLAN10 et 20 dans cet exemple).

10. Dans la partie **Plan d'adressage** > champ **Adresse IPv4**, sélectionnez l'option **IP Fixe (statique).**
11. Cliquez sur **Ajouter** et renseignez l'adresse IP et le masque réseau de l'interface GRETAP. Dans cet exemple, l'adresse IP et le réseau choisis ont pour valeur respective 192.168.44.1 (192.168.44.2 sur le firewall distant) et 255.255.255.252 :



12. Cliquez sur **Appliquer** puis **Sauvegarder** pour valider la création de l'interface GRETAP.

Créer des VLAN

Les VLAN sont d'abord créés en dehors de tout bridge avant d'être rattachés à un bridge spécifiquement créé pour leur permettre de transiter au travers du tunnel.

Sur chacun des firewalls participant au tunnel GRETAP, dans le module **Configuration** > **Réseau** > **Interfaces** :

Créer le VLAN 10 entrant

Dans le menu **Configuration** > **Réseau** > **Interfaces** :

1. Cliquez sur **Ajouter**.
2. Sélectionnez **VLAN > Sans interface parente**.
3. Placez-vous dans l'onglet **Configuration Générale.**
4. Dans la partie **État**, placez le curseur sur **ON.**
5. Dans la partie **Paramètres généraux** > champ **Nom**, indiquez un nom pour le VLAN (*vlan_10_1* dans l'exemple).
6. Dans la partie **Paramètres généraux** > champ **Interface parente**, sélectionnez l'interface portant le VLAN en entrée (interface *in* dans l'exemple).
7. Dans la partie **Paramètres généraux** > champ **Identifiant**, sélectionnez l'identifiant 802.1q associé au VLAN (*10* dans l'exemple).
8. Dans la partie **Paramètres généraux** > champ **Cette interface est** : sélectionnez **Interne (protégée)**.
9. Dans la partie **Plan d'adressage** : laissez **Dynamique / Statique** pour le champ **Adressage** et **IP dynamique (obtenue par DHCP)** pour le champ **Adresse IPv4**.
10. Cliquez sur **Appliquer**.

Créer le VLAN 10 sortant

Dans le menu **Configuration** > **Réseau** > **Interfaces** :

1. Cliquez sur **Ajouter**.
2. Sélectionnez **VLAN > Sans interface parente**.
3. Placez-vous dans l'onglet **Configuration Générale.**
4. Dans la partie **État**, placez le curseur sur **ON.**
5. Dans la partie **Paramètres généraux** > champ **Nom**, indiquez un nom pour le VLAN (*vlan_10_2* dans l'exemple).
6. Dans la partie **Paramètres généraux** > champ **Interface parente**, sélectionnez l'interface portant le VLAN en sortie (interface *Gretap_VLAN* dans l'exemple).
7. Dans la partie **Paramètres généraux** > champ **Identifiant**, sélectionnez l'identifiant 802.1q associé au VLAN (*10* dans l'exemple).
8. Dans la partie **Paramètres généraux** > champ **Cette interface est** : sélectionnez **Interne (protégée)**.
9. Dans la partie **Plan d'adressage** : laissez **Dynamique / Statique** pour le champ **Adressage** et **IP dynamique (obtenue par DHCP)** pour le champ **Adresse IPv4**.
10. Cliquez sur **Appliquer**.

Rattacher les deux VLAN à un bridge dédié

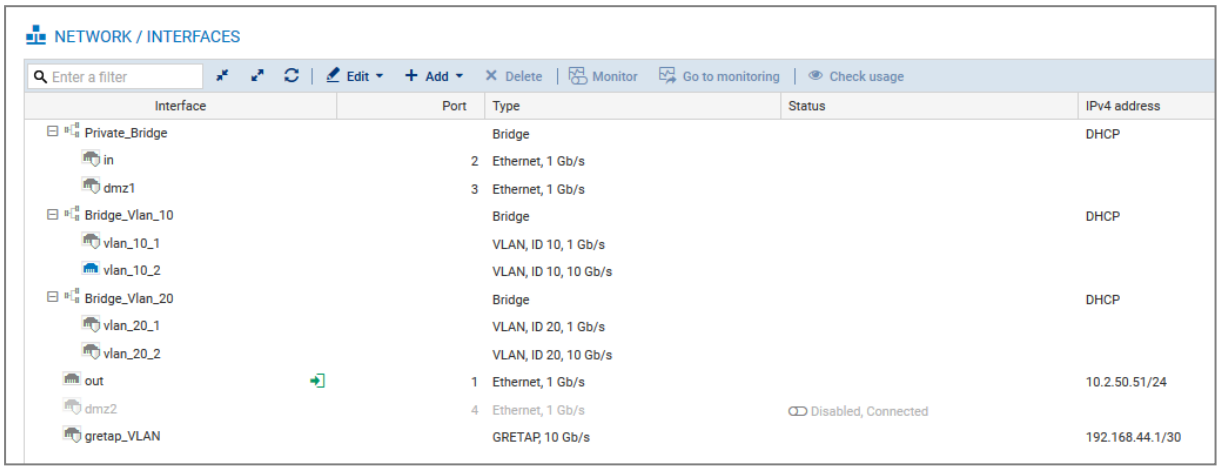
Dans le menu **Configuration** > **Réseau** > **Interfaces** :

1. Sélectionnez vlan_10_1 et vlan_10_2 dans la liste des interfaces.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Bridge** > **Avec vlan_10_1, vlan_10_2**.
4. **Nom** : précisez le nom du bridge (BridgeVlan10 dans l'exemple).
5. **Adresse IPv4** : laissez **IP dynamique (obtenue par DHCP).**
6. Cliquez sur **Appliquer**.

Créer le VLAN 20

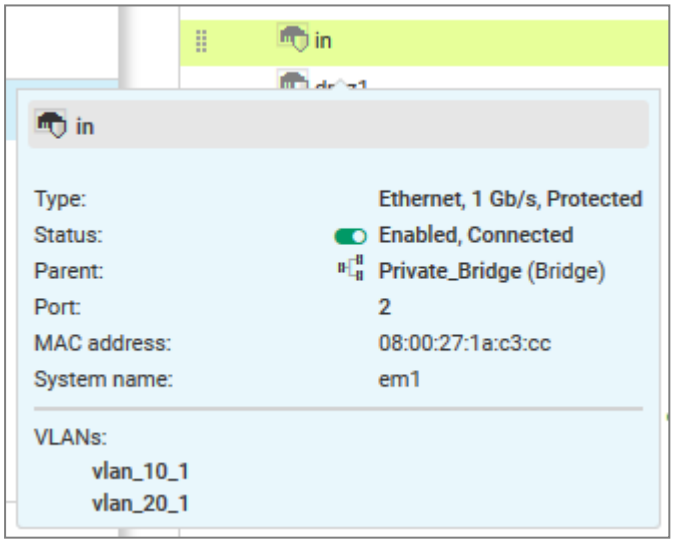
En suivant la méthode décrite précédemment, créez les vlan_20_1 et vlan_20_2 portant l'identifiant *20*, rattachés respectivement aux interfaces *in* et *gretap_VLAN* puis placés sous un nouveau bridge dédié nommé *BridgeVlan20* dans l'exemple.

Les bridges et leurs VLAN rattachés apparaissent alors dans la liste des interfaces :

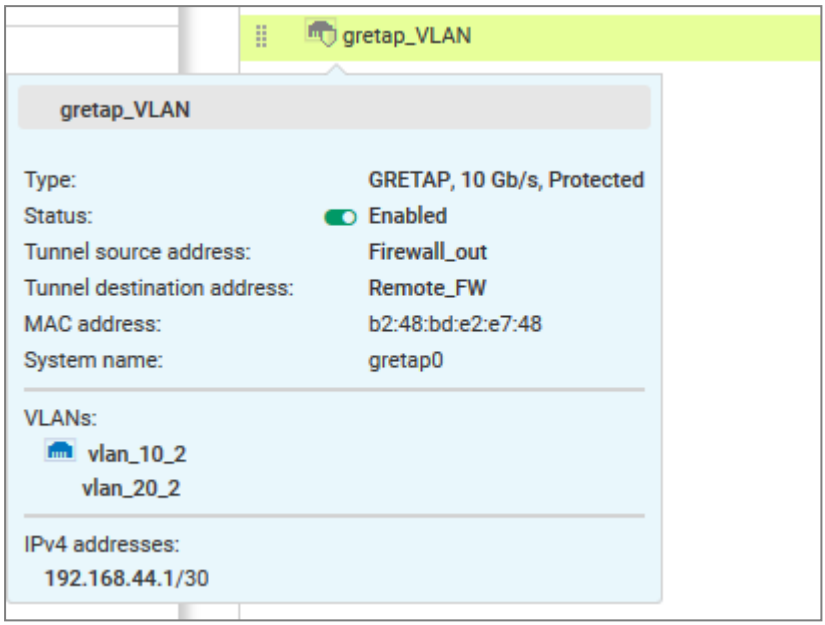


Interface	Port	Type	Status	IPv4 address
Private_Bridge		Bridge		DHCP
in	2	Ethernet, 1 Gb/s		
dmz1	3	Ethernet, 1 Gb/s		
Bridge_Vlan_10		Bridge		DHCP
vlan_10_1		VLAN, ID 10, 1 Gb/s		
vlan_10_2		VLAN, ID 10, 10 Gb/s		
Bridge_Vlan_20		Bridge		DHCP
vlan_20_1		VLAN, ID 20, 1 Gb/s		
vlan_20_2		VLAN, ID 20, 10 Gb/s		
out	1	Ethernet, 1 Gb/s		10.2.50.51/24
dmz2	4	Ethernet, 1 Gb/s	Disabled, Connected	
gretap_VLAN		GRETAP, 10 Gb/s		192.168.44.1/30

En survolant l'interface *in*, il est possible de vérifier que les VLAN *vlan_10_1* et *vlan_20_1* lui sont bien rattachés :



De même pour l'interface *gretap_VLAN* et les VLAN *vlan_10_2* et *vlan_20_2* :



Créer le tunnel IPsec

Sur chacun des firewalls participant au tunnel GRETAP, dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - Tunnels** :

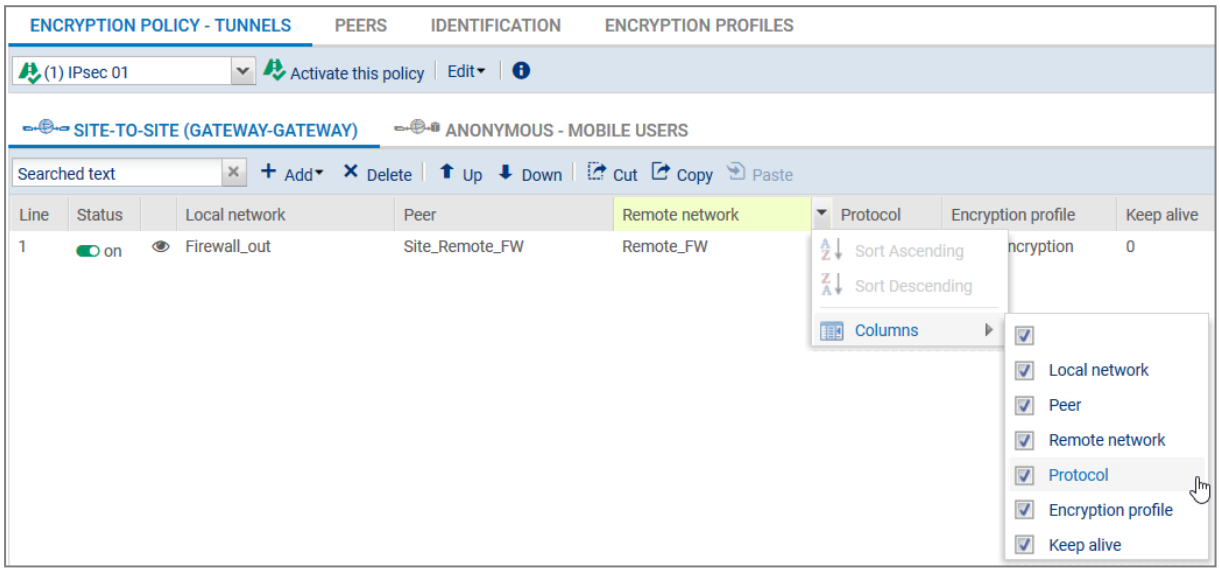
1. Cliquez sur le bouton **Ajouter.**
2. Sélectionnez **Tunnel site à site**.
3. Pour le champ **Réseau local** : sélectionnez l'interface physique portant le tunnel GRE (**Firewall_out** dans l'exemple).
4. Pour le champ **Réseau distant** : sélectionnez un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).
5. Pour le champ **Choix du correspondant** : créez (ou sélectionnez-le s'il existe déjà) un correspondant dont la passerelle distante sera un objet portant l'adresse IP publique du Firewall distant.
6. Cliquez sur **Terminer**.

NOTES
Pour plus de détails concernant la création d'un correspondant utilisant les méthodes d'authentification par clé pré-partagée ou par certificats, veuillez consulter les documents VPN IPsec - Authentification par clé pré-partagée et VPN IPsec - Authentification par certificats.

La version du protocole IKE pour ce correspondant doit être identique à :

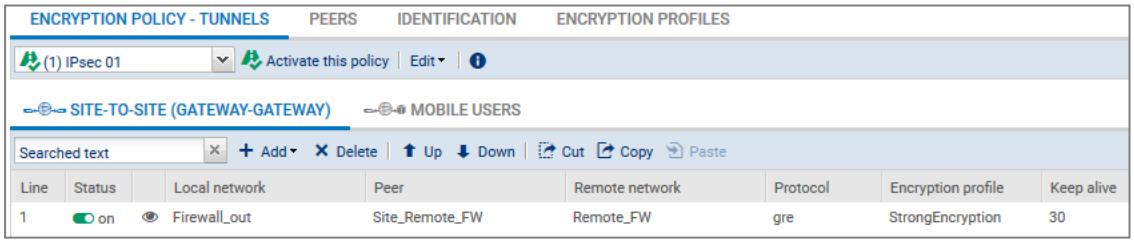
- Celle utilisée sur le firewall distant,
- Celle des correspondants utilisés dans les autres règles de la politique IPsec concernée.

1. Afin de ne pas autoriser l'établissement du tunnel IPsec pour des protocoles autres que GRE et éviter le chiffrement de flux tels que ICMP (*Ping*), il est conseillé de spécifier le protocole GRE dans la colonne **Protocole**.
   Si cette colonne n'est pas affichée, passez votre souris sur le titre d'une colonne quelconque et déroulez le menu contextuel en cliquant sur la flèche. Sélectionnez **Colonnes** puis cochez **Protocole**.



2. Pour permettre au tunnel de s'établir sans flux initial et de rester établi même lorsque le trafic s'interrompt pour une courte période, cliquez dans la colonne **Keepalive** et choisissez une durée (30 secondes dans l'exemple).

La politique VPN IPsec prendra donc la forme suivante :



NOTE
Le firewall étant à l'initiative de l'émission des paquets réseau GRE, il n'est donc pas nécessaire de créer de règles de filtrage pour ce protocole.

Vérifier le fonctionnement

Depuis une machine du site A appartenant à l'un des VLAN, faites un test de disponibilité (*Ping*) vers une machine du site B appartenant au même VLAN : la machine du site B doit répondre aux requêtes.

Il est également possible de vérifier que les VLAN sont bien transportés dans le tunnel en effectuant une capture réseau sur l'interface d'entrée du tunnel du firewall du site B. Dans ce cas, les paquets réseaux capturés laissent ainsi apparaître le protocole GRE encapsulant le VLAN transporté (VLAN 20 dans l'exemple):

```
15:41:06.019669 00:90:fb:2c:5d:b2 > 00:0d:b4:0c:c6:b6, ethertype IPv4 (0x0800), length 108: 172.16.3.1 > 172.16.2.1: GREv0,
proto TEB (0x6558), length 74: 18:03:73:8b:51:d8 > 01:00:5e:00:00:fc, ethertype 802.1Q (0x8100), length 70: vlan 20, p 0,
ethertype IPv4, 192.168.1.10.50677 > 224.0.0.252.5355: UDP, length 24
```

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu